VERIFICATION OF TRANSLATION

I, Toyoaki Fukui, translator of FUKUI & PARTNER of 1-19, Uchihonmachi 2-chome, Chuo-ku, Osaka-shi, Osaka, JAPAN, do hereby solemnly and sincerely declare as follows:

1. That I have a competent knowledge of the English and Japanese Languages.
2. That the attached document entitled:

   "COPYING APPARATUS"

   is a true and correct translation in English of a Japanese Patent Application No. 11-049996 filed on February 26, 1999.

DATED This 2nd day of June, 2003.

T. Fukui

Toyoaki Fukui
Translator

PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: February 26, 1999

Application Number: Patent Application 11-049996

Applicant(s): Matsushita Electric Industrial Co., Ltd.

March 3, 2000

Commissioner,

Japan Patent Office Takahiko Kondoh

Certification No. 2000-3012824

[Document Name] Patent Request

[Docket Number] 2036610016

[Date of Filing] February 26, 1999

[Address] Commissioner of the Patent Office

[IPC] H04N 1/00

[Inventor]

[Residence or Address] c/o Matsushita Electric Industrial Co., Ltd, 1006, Oaza Kadoma, Kadoma-shi, Osaka

[Name] Akio Kojima

[Inventor]

[Residence or Address] c/o Matsushita Electric Industrial Co., Ltd, 1006, Oaza Kadoma, Kadoma-shi, Osaka

[Name] Yasuhiro Kuwahara

[Inventor]

[Residence or Address] c/o Matsushita Electric Industrial Co., Ltd, 1006, Oaza Kadoma, Kadoma-shi, Osaka

[Name] Tatsumi Watanabe

[Applicant]

[ID Number] 000005821

[Name] Matsushita Electric Industrial Co., Ltd.

[Agent]

[ID Number] 100097445

[Patent Attorney]

[Name] Fumio Iwasaki

[Elected Agent]

[ID Number] 100103355

[Patent Attorney]

[Name] Tomoyasu Sakaguchi

[Elected Agent]

[ID Number] 100109667

[Patent Attorney]

[Name] Hiroki Naitoh

[Expression of Fee]

[Deposit Account No.] 011305

[Amount of payment] 21,000 yen

[List of Attached Articles]

[Document Name]	Specification	1
[Document Name]	Drawings	1
[Document Name]	Abstract	1

[Number of General Power of Attorney] 9809938

[Proof request] No

[Name of The Document] Specification

[Title of The Invention] Copying Apparatus

[Claims]

1. A copying apparatus comprising:

target data to be copied;

copy-inhibition information comprising data for which copying is prohibited;

a data-monitoring means of monitoring the image created from said target data based on said copy-inhibition information;

a copying means of creating a copy of said target data;

an information-registration means of registering said copy-inhibition information; and

a control means of performing control such that the copying operation is stopped when said created image is considered to be said copy-inhibition information.

2. The copying apparatus of claim 1 wherein said copy-inhibition information is provided using memory media.

3. The copying apparatus of claim 1 wherein said copy-inhibition information is provided over the network.

4. A copying apparatus comprising:

target data to be copied;

a first specific-information-extraction means of extracting

identification information unique to a specified apparatus related to said copy data; and

an information-addition means of adding said identification information to said target data and creating new copy data.

5. The copying apparatus of claim 4 wherein said identification information is chip ID information given to the central processing unit (CPU).

6. The copying apparatus of claim 4 wherein said identification information is the IP address given to an apparatus.

7. A copying apparatus comprising:

target data to be copied;

a second specific-information-extraction means of extracting specific application information that is unique to the software related to said copy data; and

an information-addition means of adding said specific application information to said target data and creating new copy data.

8. The copying apparatus of claim 7 wherein said specific application information is a mail address set by the user.

9. A copying apparatus that receives copy data and creates a copy according to that copy data and comprises:

an extraction means of analyzing said copy data and extracting unique information that specifies a specific apparatus that is related to the

copy data; and

a specific-information-addition means of adding the extracted unique information to the copy as new copy data.

10. The copying apparatus of claim 9 wherein said specific apparatus has an ID number that can specify a personal computer.

11. The copying apparatus of claim 10 wherein said identification information is an IP address that is given to the apparatus.

12. A copying apparatus that receives copy data and creates a copy according to that copy data and comprises:

an extraction means of analyzing said copy data and extracting unique information that specifies software that is related to the copy data; and

a specific-information-addition means of adding the extracted unique information to the copy as new copy data.

13. The copying apparatus of claim 12 wherein said unique information is a mail address set by the user.

14. The copying apparatus of claim 12 wherein said unique information is registration information for the software.

15. A copying apparatus that corresponds to a network and receives copy data and creates a copy according to the copy data and comprises:

an extraction means of extracting the IP address that is given to said

copying apparatus; and

a specific-information-addition means of adding the extracted IP address to the copy as new copy data.

[Background of the Invention]

[0001]

[Field of the Invention]

This invention relates to a copying apparatus that prevents illegal copying of confidential documents, confidential data, or copyrighted materials such as confidential data, documents, videos, printed material, paper money, stocks and bonds and all kinds of cash certificates for which copying is prohibited.

[0002]

[Description of the Related Art]

In recent years, with the advancement of networking and digitization, personal devices are being connected to networks in order to more easily obtain and print electronic data. However, as a result of DTP technology that is being developed with the objective of creating images that are true to the original document, it is possible to obtain more accurate copied materials. This is creating an environment in which is easy to obtain electronic data and to perform more accurate copying.

[0003]

On the other hand, when documents that are to be handled confidentially are copied, problems occur such as in secrecy leaks.

Moreover, if it were possible to easily obtain copies that cannot be distinguished from the original document, there is a possibility that there would be more illegal use of copyrighted materials, and that copies would be used for counterfeiting of paper money and stocks and bonds, making damage large.

[0004]

Conventionally, color copiers have been equipped with an anti-counterfeiting function to prevent counterfeiting paper money or the like. Fig. 9 is a block diagram of this kind of conventional color copier. In Fig. 9, counterfeiting is prevented by a specific-image-judgment circuit 120 that uses features of an image to determine whether the image signal that is read from the scanner 110 is an image signal for paper money or a stock or bond for which copying is prohibited, and then activates a copy-protection function that reproduces the image after performing a conversion process such as image compression or reflected image inversion, and performs a process to make it possible to easily recognize that the copied material is a copy before outputting the copy to the printer 130 (for example, the image processing apparatus disclosed in Japanese patent No. H1-316783).

[0005]

[Problems to Be Solved By the Invention]

One remarkable recent trend is not only the spread of paper copies, but also the spread of digitized documents. There is a problem, in that with the use of a personal computer, it is easy to obtain confidential electronic documents and copyrighted data over a network, and to perform

a large quantity of illegal copying using a high-speed printer.

[0006]

However, this prior technology judges the image of the document read by the scanner, but does not deal with the problem related to electronic data that are read from the scanner.

[0007]

The object of this invention is to solve the aforementioned problem by providing a data monitoring method that avoids and quickly prevents illegal copying of copying-prohibited electronic data.

[0008]

[Means For Solving the Problem]

In order to solve the problem mentioned above, a first copying apparatus of the present invention, comprises: target data to be copied; copy-inhibition information comprising data for which copying is prohibited; a data-monitoring means of monitoring the image created from the target data based on the copy-inhibition information; a copying means of creating a copy of the target data; an information registration means of registering the copy-inhibition information; and a control means of performing control such that the copying operation is stopped when the created image is considered to be copy-inhibition information.

[0009]

Also, a second copying apparatus of the invention comprises: target data to be copied; a first specific-information-extraction means of

extracting identification information unique to a specified apparatus related to the copy data; and an information-addition means of adding the identification information to the target data and creating new copy data.

[0010]

Also, a third copying apparatus of this invention comprises; target data to be copied; a second specific-information-extraction means of extracting specific application information that is unique to the software related to the copy data; and an information-addition means of adding the specific application information to the target data and creating new copy data.

[0011]

Moreover, a fourth copying apparatus of this invention is a copying apparatus that receives copy data and creates a copy according to that copy data and comprises: an extraction means of analyzing the copy data and extracting unique information that specifies a specific apparatus that is related to the copy data; and a specific-information-addition means of adding the extracted unique information to the copy as new copy data.

[0012]

Also, a fifth copying apparatus of this invention is a copying apparatus that receives copy data and creates a copy according to that copy data and comprises: an extraction means of analyzing the copy data and extracting unique information that specifies software that is related to the copy data; and a specific-information-addition means of adding the extracted unique information to the copy as new copy data.

[0013]

Also, a sixth copying apparatus of the invention is a copying apparatus that corresponds to a network and receives copy data and creates a copy according to the copy data and comprises: an extraction means of extracting the IP address that is given to the copying apparatus; and a specific-information-addition means of adding the extracted IP address to the copy as new copy data.

[0014]

[Description of the Preferred Embodiments]

The preferred embodiments of the invention will be explained below with reference to the drawings.

[0015]

(First Embodiment)

First, Fig. 1, Fig. 2, Fig. 3 and Fig. 4 will be used to explain a first embodiment of the invention, which is an example of a copying apparatus that prohibits illegal copying by a personal computer.

[0016]

Fig. 2 shows the operating environment of the personal computer. The personal computer 1 (hereafter referred to as PC 1) is installed with application software, and when configured with a simple printing system, it performs editing, processing and image processing (color processing). A scanner 3 is used for inputting images to the PC 1. A printer 2 creates a printed image according to printing data from the PC 1 on normal paper or

OHP paper. By connecting the PC 1 to a network 100, it is possible to obtain images from a network scanner 5 (hereafter referred to as NS 5) over the network 100, and to transfer printing data to a network printer 4 (hereafter referred to as NP 4) to print the data. A DTP system can also constructed with a PC1 that performs color processing and other processing, and a printer 2 that performs printing. Furthermore, a scanner 3 for reading images can is connected.

[0017]

Next, Fig. 1 will be used to explain the operation when the PC 1 prints specific printing data.

[0018]

Fig. 1 is a block diagram of a personal computer 1. The PC 1 specifies printing after the application software installed in the PC 1 sets the printing image, and creates printing data 11. The PC 1 also transfers the printing data 11 to the printer driver 12. The printer driver 12 is pre-installed in the PC 1 as a control program for transferring data to the printer 2. The printer driver 12 transfers the printing data 11 that are specified for printing by the application software to the printer 2.

[0019]

A printing-information-analyzing circuit 15 constantly monitors the printing data 11 that are transferred to the printer 2, and creates a final image in the confirmation memory 16 using character-string information that is given using page notation language, image-pattern information, code information, and encryption information that is embedded using

electronic-watermarking technology, and compares and analyzes it with copy-inhibition information 14. In the case that the printing information for the printing data 11 is determined to have been pre-registered in the printing-prohibited information 14, the printing-information-analyzing circuit 15 outputs a stop instruction 151 to the printer driver 12 to stop transferring printing data. The printer driver 12 stops transferring printing data according to the stop instruction 151. In this way, it is possible to prevent illegal printing on the PC 1 level.

[0020]

The contents of the copy-inhibition information 14 can be constantly updated according to contents for which printing is to be prohibited. In this way, it is possible to keep the contents quickly updated such that they correspond with the daily changing secrecy management level, confidential information, and anti-counterfeiting technology and encryption technology whose development is always progressing. This update method will be explained. When an information card 210 is inserted, an information-registration circuit 81 verifies the information card 210, and only when it is determined that there is authorization to perform registration, will the registration data saved on the information card 210 be obtained. Next, the information-registration circuit 81 rewrites the contents of the copy-inhibition information 14 based on the obtained registration data. It is also possible to obtain the registration data via a network 100. By having this remote registration function, it is possible to easily update the printing-prohibited information, and to daily update the contents with the most recent information. Since it is not necessary to replace the internal memory of the apparatus, updating can be performed

quickly and it is possible to prevent the spread of illegal copying from increasing.

[0021]

Also, by performing a verification check, it is possible to prevent someone from changing the information and performing illegal printing. Moreover, it is possible to have management levels, and to manage confidential information on various levels.

[0022]

The information card 210 can be an IC card, FD (floppy disk), CD-ROM, DVD-RAM or the like, as long as it is recording media on which information can be registered. Next, Fig. 3 will be used to explain the information contained in the copy-inhibition information 14. Fig. 3 shows the information contained in the copy-inhibition information 14.

[0023]

Information that is capable of specifying a document such as character information 141 for the document data, image-pattern information 142, code information, and encryption information 144 that is embedded in the image using electronic watermarking technology is saved as copy-inhibition information.

[0024]

The title of the document and special character strings used in the document (for example, major keywords used in a confidential document) are saved in the character information 141 for the document data.

Unique pattern information that is capable of specifying the printing information is saved in the image-pattern information 142. When a document-management code is given to the original document data, analysis information for the corresponding code is saved in the code information 143. Decoding information for decoding the electronic watermark embedded in the photo-image data protected by a copyright, an decoding algorithm for decoding the encryption patter that is printed according to a pre-specified encryption (such as security printing, etc.) on the original document that is read by the scanner 3, and code-type information are saved in the encryption information. The copy-inhibition information 14 can be any information that can specify the printing information for all kinds of printed materials such as paper money, stocks and bonds, money certificates, and the like.

[0025]

Next, Fig. 4 will be used to explain the operation of the printing-information-analysis circuit 15. Fig. 4 is a block diagram of the printing-information-analysis circuit 15. The printing-information-analysis circuit 15 constantly monitors the printer driver 12 and always performs a specified operation when printing starts. First, when the operation starts, a drawing engine 154 obtains the drawing information of the printing data 11 from the printer driver 12, and performs the drawing operation according to the drawing information in the confirmation memory 16. The contents of the drawn drawing-image data 161 are analyzed by various analyzing engines. The title-analyzing engine 155 specifies the title region in the drawing-image data 161 and transfers the analysis results of those contents to the collating circuit 159. The

collating circuit 159 selects character information 141 from the copy-inhibition information 14 that can be used as collating information, and compares it with the analysis results that were transferred by the title-analyzing engine 155. When the comparison results show that there is matching information, the printing is regarded as printing of an illegal copy, and the collating circuit 159 stops the printing operation of the printer driver 12 by signal 151.

[0026]

Similarly, the document-analyzing engine 156 detects and analyses the text region, the image-analyzing engine 157 detects and analyzes the photo region, and the code-analyzing engine 158 detects and analyzes the code region. The analysis results from each engine are transferred to the collating circuit 159. The collating circuit 159 selects character information 141, image-pattern information 142, code information 143 and encryption information 144 from the copy-inhibition information and compares that information with the analysis results that are transferred from each of the analyzing engines. When any of the results show that there are matches, the printing is regarded as printing of an illegal copy, and the collating circuit 159 stops the printing operation of the printer driver 12 by the signal 151. Also, the code-analyzing engine 158 could be such that it requests the necessary decoding algorithm for decoding from the collating circuit 159 and obtains the latest decoding algorithm. In this way, it is possible to always keep current with the latest encryption technology. The collating circuit 159 obtains the necessary information from the copy-inhibition information 14 according to requests from the analyzing engines and sends that information to the respective analyzing

engines.

[0027]

By having a plurality of analyzing engines in this way, it is possible to correspond to printed documents having various different document characteristics.

[0028]

With the first embodiment described above, by having a function that analyses the printing contents sent from the PC 1 to the printer when printing and prevents illegal copying, it is possible to prevent illegal copying of in-house confidential documents, and prevent counterfeiting of paper money and the like. Furthermore, by having a method that is capable of easily updating copy-inhibition information, it is possible to quickly correspond to daily changes in secrecy management levels, confidential information, and the latest progress in the development of new anti-counterfeiting technology and encryption technology. As a result, it is possible to prevent an increase in the spread of illegal copying.

[0029]

Also, by performing a verification check, it is possible to prevent someone from changing information and performing illegal printing. Moreover, it is possible to have management levels, and to manage confidential information on various levels.

[0030]

Furthermore, in the case of providing the personal computer with a

function to prevent illegal copying, there is no need for special hardware, and only software needs to be installed, thus it is possible to reduce costs.

[0031]

(Second Embodiment)

In the first embodiment, a copying apparatus having a personal computer with a function for preventing illegal copying was explained, however, here an embodiment of a copying apparatus that identifies a device that outputs illegal copies when illegal copies begin to appear, and quickly tracks the illegal copy is explained. Fig. 5 is a block diagram of an information-addition circuit 18 that adds identification information unique to a device to the copy data.

[0032]

The information-addition circuit 18 extracts CPU ID information 18a that is stored in the central processing unit (hereafter referred to as CPU) of PC 1, and sends that information to the printer driver 19. The printer driver 19 adds the CPU ID information 18a to the printing data 11, and outputs that data to the printer 2 as new printing data. There is only one unique CPU in the PC 1, and is the information source of information that is managed by the user.

[0033]

Similarly, the information-addition circuit 18 obtains application-registration information 18b contained in the PC 1 from the application software 92, and sends that information to the printer driver. Registration information comprises user-registration information, user

information, such as mail address, of the user of the apparatus, date information, etc. The printer driver 19 adds the application-registration information 18b to the printing data, and outputs that data to the printer 2 as new printing data.

[0034]

The application-registration information 18b comprises user-registration information that is registered at the time of installation, and the registration of specific key numbers that are distributed to the user. Also, the mail address that is set by the user for the application is effective as information for tracking the address of the user, and is an effective information source of information that identifies the user, location and date related to the copy. It is also possible to used registration information of the operating system (hereafter referred to as OS) of the PC 1, or any information that can identify the user and the software by the installed software.

[0035]

Similarly, the information-addition circuit 18 extracts hardware information 18c from the PC 1 and sends that information to the printer driver 19. The printer driver 19 adds the hardware information 18c to the printing data, and outputs that data to the printer as new printing data. Information about the board on which the CPU of the PC 1 is mounted, and the IP address set by the network interface are obtained as hardware information. Also, information about the connected printer 2 can be obtained from the driver.

[0036]

With this second embodiment, by adding information identifying the user of a device or software, the location, and date to the printing data, it is possible to track the origin, date and user of the copied material. In this way it becomes possible to quickly find the device used for outputting an illegal copy, and since evidence of the conditions under which the printing data were created remain, it is possible to prevent a spread of the illegally copied material, and to keep the amount of leaked confidential information to a minimum.

[0037]

(Third Embodiment)

Here an embodiment of using a tracking function in the printer 2 will be explained. Fig. 6 will be used to explain the operation of the printer 2. Fig. 6 is a block diagram of the printer 2.

[0038]

The printer 2 receives printing data from the PC 1 in the receiving buffer 21, and sends the printing data in order to the command-analyzing circuit 22. The command-analyzing circuit 22 analyzes the language and image-data format of the received printing data.

[0039]

In addition to analyzing the language and image-data format of the received printing data, the command-analyzing circuit 22 extracts ID information 222 (apparatus information, software information, hardware information) that is added to the printing data and gives it to the

specific-information-addition circuit 80.

[0040]

Next, according to the analysis result, the command-analyzing circuit 22 transfers the printing data to the graphics/character-drawing circuit 23 when it is necessary to draw graphics. The graphics/character-drawing circuit 23 performs a specified drawing operation on the image memory 26 via the memory controller 25. Similarly, according to the analysis result, the command-analyzing circuit 22 transfers data to the image-drawing circuit 27, when it is necessary to use photo data.

[0041]

The image-drawing circuit 27 creates specified photo data in the image memory 26 via the memory controller 25.

[0042]

The specific-information-addition circuit 80 converts the ID information 222 to a specified pattern and adds it to the created image in the image memory 26 via the memory controller 25. For example, as shown in Fig. 7, a specific-information code 1000 is added to the printing data 261. It is also possible to send a specific pattern directly to the printer engine 24 and print it on paper.

[0043]

After the desired image data are formed in the image memory 26, the memory controller transfers that image data to the printer engine 24. The printer engine 24 then performs printing on paper from the received

image data.

[0044]

With this third embodiment, specific information that was added to the printing data received by the printer 2 is extracted, and when performing printing inside the printer 2, that specific information is then further added to the printing data automatically, so it is possible to track the device used when in the case of illegal copying of in-house confidential documents occurs, or when counterfeiting of paper money and the like is performed.

[0045]

(Fourth Embodiment)

Here, an embodiment will be explained in which the printer 4 that is connected to a network has a tracking function. Fig. 8 will be used to explain the operation of the printer 4. Fig. 8 is a block diagram of the printer 4.

[0046]

The printer 4 receives printing data from the PC 1 via a network interface 41, and sends the data in order to the command-analyzing circuit 42. The command-analyzing circuit 42 analyzes the language and image-data format of the received printing data.

[0047]

Next, according to the analysis results, the command-analyzing circuit 42 transfers the printing data to the graphics/character-drawing

circuit 43 when it is necessary to draw graphics. The graphics/character-drawing circuit 43 performs a specified drawing operation in the image memory 46 via the memory controller 45. Similarly, according to the analysis results, the command-analyzing circuit 42 transfers the printing data to the image-drawing circuit 47 when it is necessary to create photo data.

[0048]

The image-drawing circuit 47 creates specified photo data in the image memory 46 via the memory controller 45.

[0049]

The specific-information-addition circuit 80 extracts the IP address 223 given to the printer 4 from the network interface 41, and coverts that IP address to a specific pattern and adds it to the image in the image memory 46 via the memory controller 45. The form that this pattern is added can be as in the third embodiment where specific-information code is added to the printing data as shown in Fig. 7. It is also possible to send the specific pattern directly to the printer engine 33 and print it on paper.

[0050]

After the desired image data are formed in the image memory, the memory controller 45 transfers that image data to the printer engine 44. The printer engine 44 then prints the image from the received image data on paper.

[0051]

With this fourth embodiment, the ID information (IP address) of the printer 4 that is connected to the network is automatically added to the printing data when printing inside the printer 4, so it is possible to easily identify and track the source of printing when a confidential document is printed illegally in house, or when counterfeiting of paper money or the like is performed.

[0052]

The copying apparatus of this invention can be realized through the use of CPU and DSP software. It can also be realized by special hardware.

[0053]

Of course it is also possible to used document exchange software such as database software, distribution-system software or electronic-mail software, or document distribution software as the confidential-document-management software.

[0054]

Also, the invention is not limited to still images, but can be applied in the same way to video images, and the invention can be used for managing video-data.

[0055]

[Effect of the Invention]

As described above, with this invention, it is possible to avoid or quickly prevent illegal copying of documents, electronic mail, or the like

for which copying is prevented.

[0056]

Also, information unique to the apparatus or application used is added automatically to the printed material so it is possible to identify the apparatus on which illegal copying was performed, and prevent the spread of confidential information.

[Brief Explanation of the Drawings]

Fig. 1 is a block diagram of the personal computer 1 of a first embodiment of the invention.

Fig. 2 is a schematic drawing showing the operating environment of the personal computer of the first embodiment of the invention.

Fig. 3 is a drawing showing the information contained in the copy-inhibition information 14 of the first embodiment of the invention.

Fig. 4 is a block diagram of the printing-information-analyzing circuit 15 of the first embodiment of the invention.

Fig. 5 is a block diagram of the information-addition circuit 18 of a second embodiment of the invention.

Fig. 6 is a block diagram of the printer 2 of a third embodiment of the invention.

Fig. 7 is a drawing explaining the printing data 261 of the third embodiment of the invention.

Fig. 8 is a block diagram of the printer 4 of a fourth embodiment of the invention.

Fig. 9 is a block diagram of a prior color copy machine.

[Explanation of the Reference Numbers]

1 Personal computer

2 Printer

3 Scanner

4 Network printer

5 Network scanner

11 Printing data

12 Printer driver

13 Information updating circuit

14 Copy inhibition data

15 Printing information analyzing circuit

16 Confirmation memory

18 Information addition circuit

18a CPU ID information

18b Application registration information

18c Hardware information

21 Receiving buffer

22 Command analyzing circuit

23 Graphic/character drawing circuit

24 Printer engine

25 Memory controller

26 Image memory

27 Image drawing circuit

28 Printing information analyzing circuit

29 Copy inhibition information

41 Network interface

42 Command analyzing circuit

43 Graphic/character drawing circuit

44 Printer engine

45 Memory controller

46 Image memory

47 Image drawing circuit

80 Specific information addition circuit

81 Information registration circuit

91 CPU

92 Application

93 Network interface

100 Network

210 Information card

222 ID information

223 IP address

261 Printing data

1000 Specific information code

Fig. 1

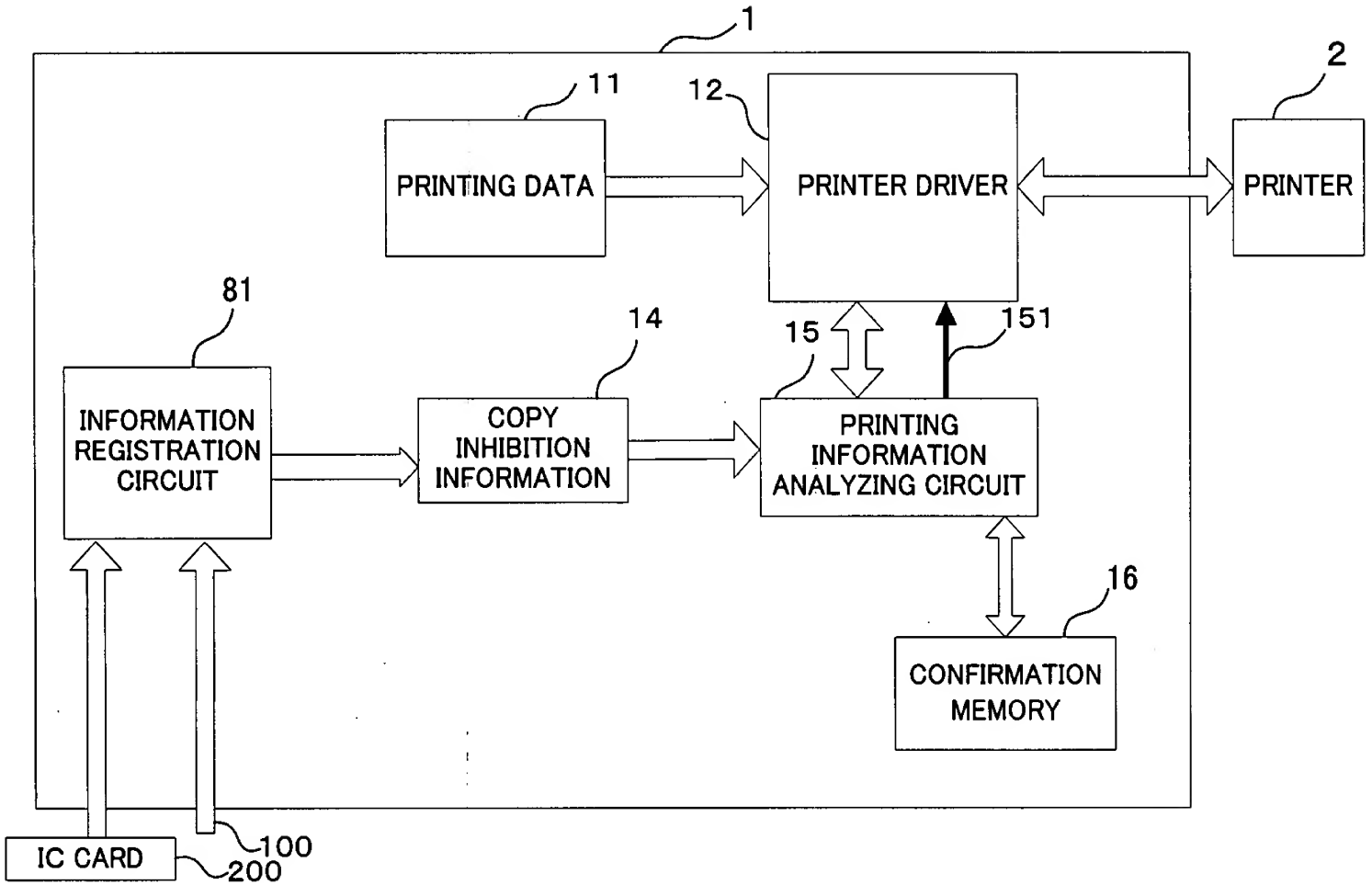

1
2
11
12
PRINTING DATA
PRINTER DRIVER
PRINTER
81
14
15
151
INFORMATION REGISTRATION CIRCUIT
COPY INHIBITION INFORMATION
PRINTING INFORMATION ANALYZING CIRCUIT
16
CONFIRMATION MEMORY
IC CARD
100
200

Fig. 2

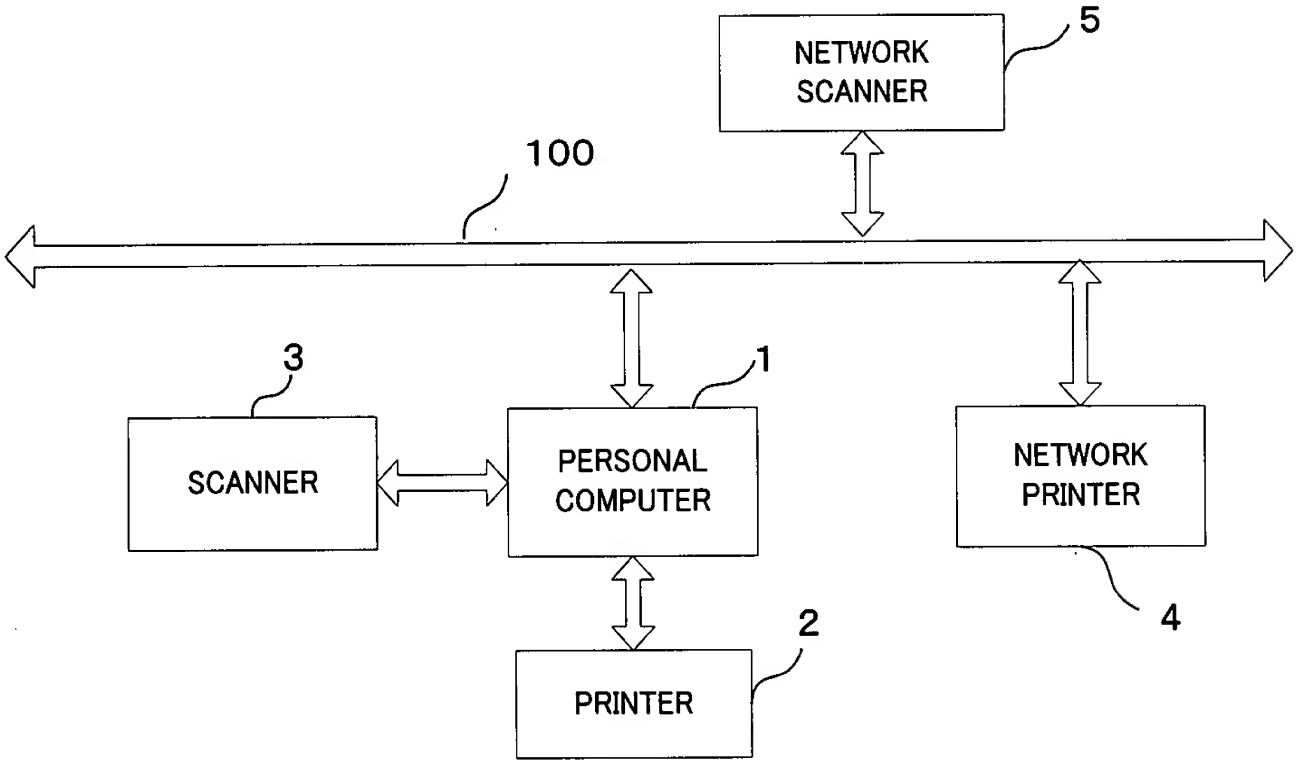

NETWORK SCANNER
5
100
3
1
SCANNER
PERSONAL COMPUTER
NETWORK PRINTER
4
2
PRINTER

Fig. 3

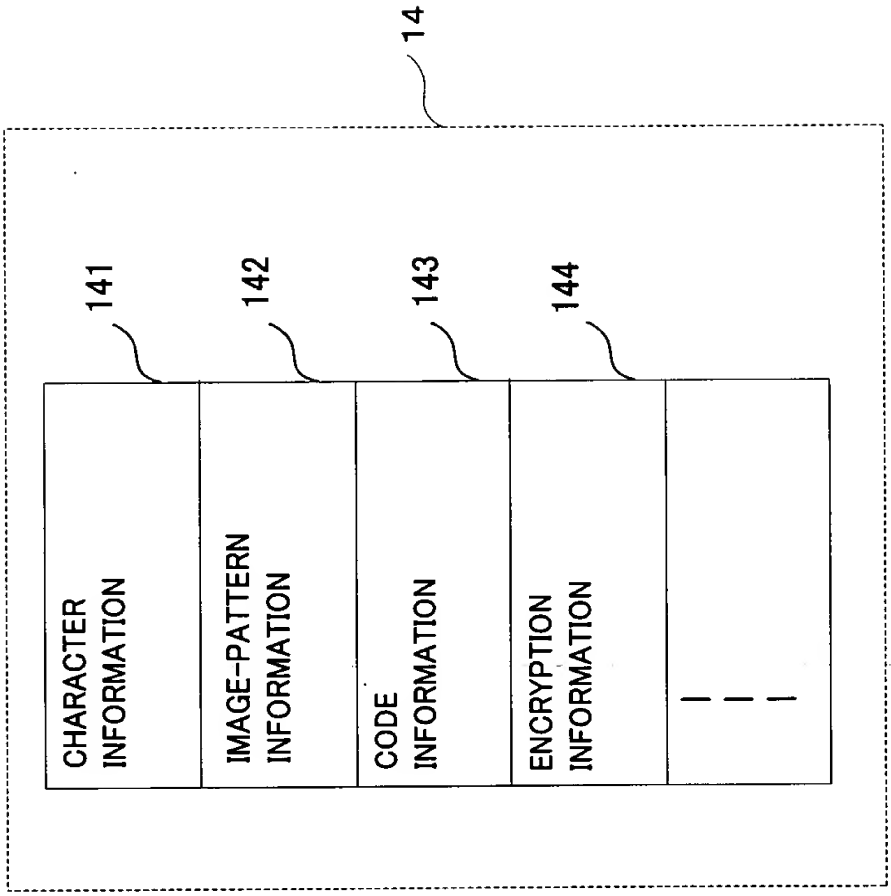

14
141
142
143
144
CHARACTER INFORMATION
IMAGE-PATTERN INFORMATION
CODE INFORMATION
ENCRYPTION INFORMATION

Fig. 4

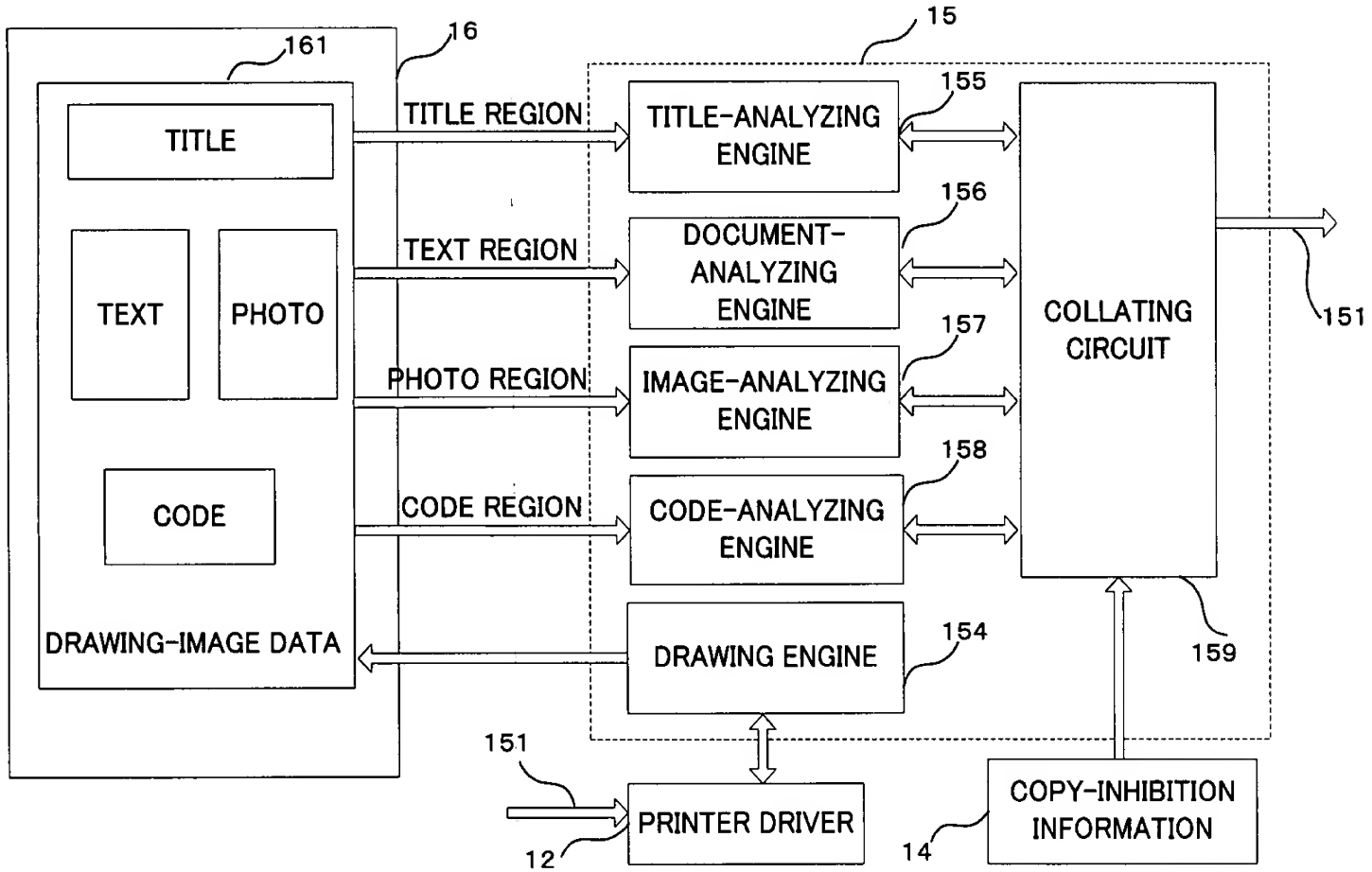

161
16
15
TITLE
TEXT
PHOTO
CODE
DRAWING-IMAGE DATA
TITLE REGION
TEXT REGION
PHOTO REGION
CODE REGION
TITLE-ANALYZING ENGINE
155
DOCUMENT-ANALYZING ENGINE
156
IMAGE-ANALYZING ENGINE
157
CODE-ANALYZING ENGINE
158
DRAWING ENGINE
154
COLLATING CIRCUIT
151
159
151
PRINTER DRIVER
12
COPY-INHIBITION INFORMATION
14

Fig. 5

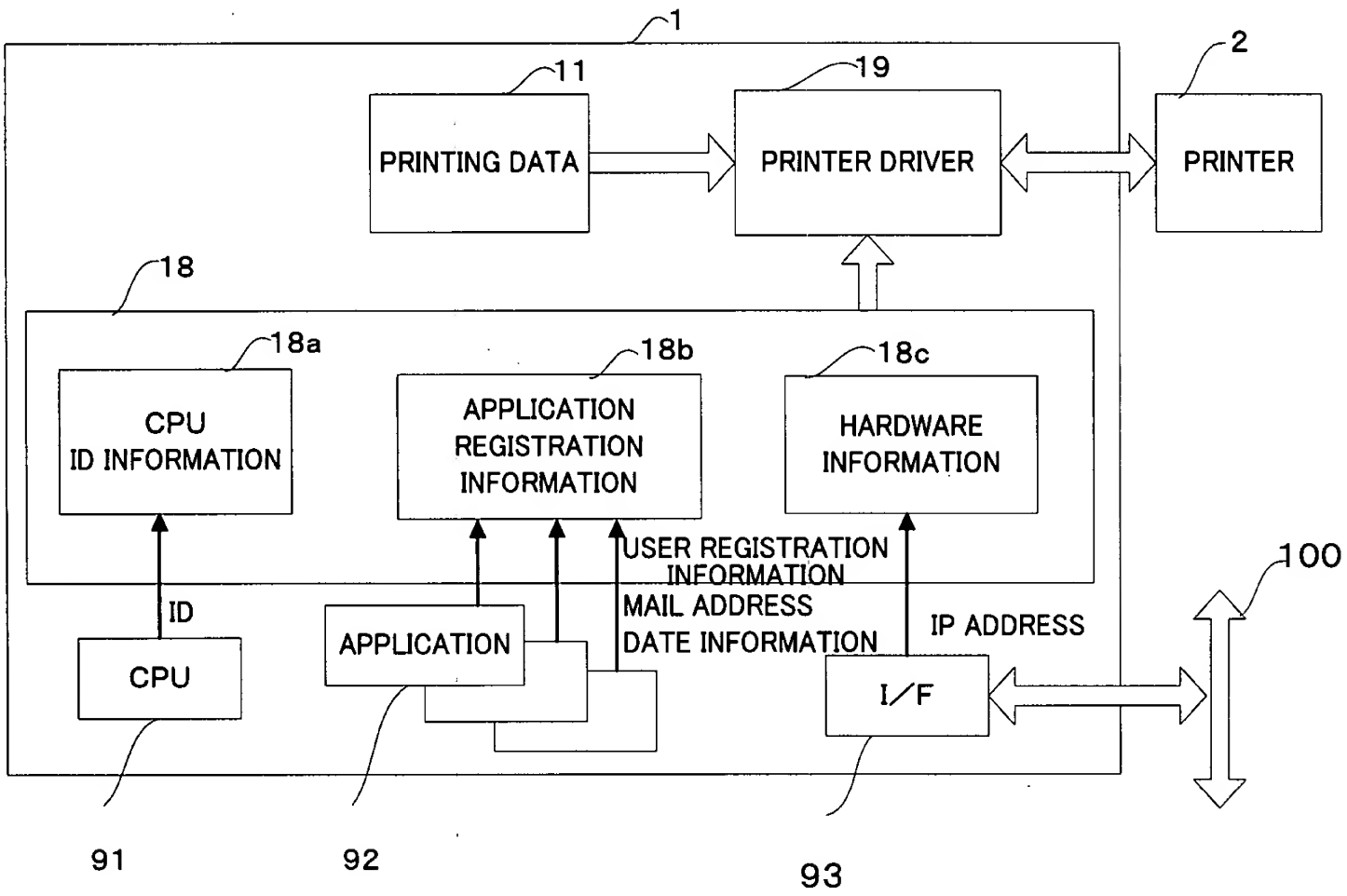

1
2
11
19
PRINTING DATA
PRINTER DRIVER
PRINTER
18
18a
18b
18c
CPU
ID INFORMATION
APPLICATION
REGISTRATION
INFORMATION
HARDWARE
INFORMATION
USER REGISTRATION
INFORMATION
MAIL ADDRESS
DATE INFORMATION
IP ADDRESS
100
ID
CPU
APPLICATION
I/F
91
92
93

Fig. 6

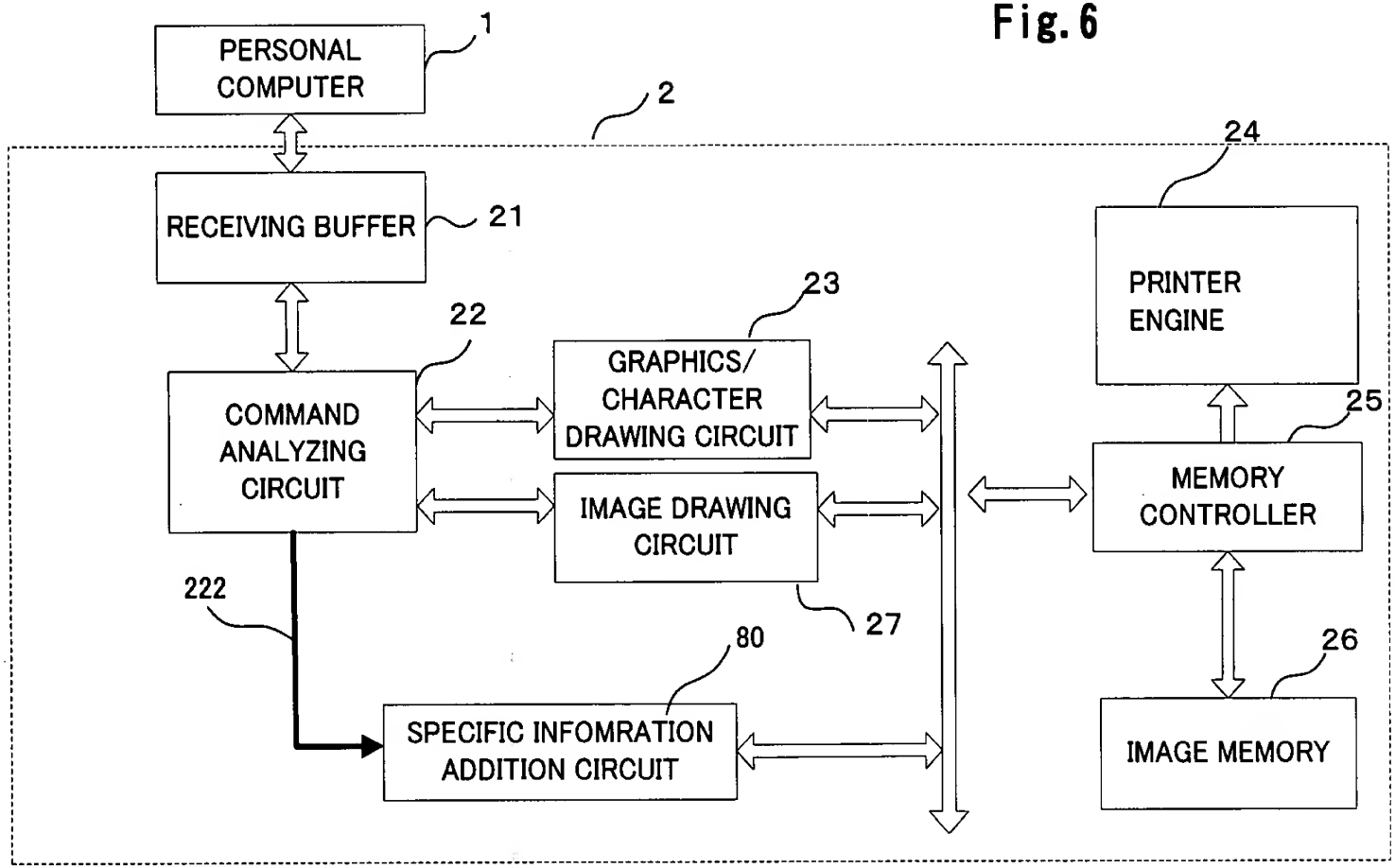

PERSONAL COMPUTER
1
2
RECEIVING BUFFER
21
22
23
24
COMMAND ANALYZING CIRCUIT
GRAPHICS/ CHARACTER DRAWING CIRCUIT
IMAGE DRAWING CIRCUIT
PRINTER ENGINE
25
MEMORY CONTROLLER
222
27
80
26
SPECIFIC INFOMRATION ADDITION CIRCUIT
IMAGE MEMORY

Fig. 7

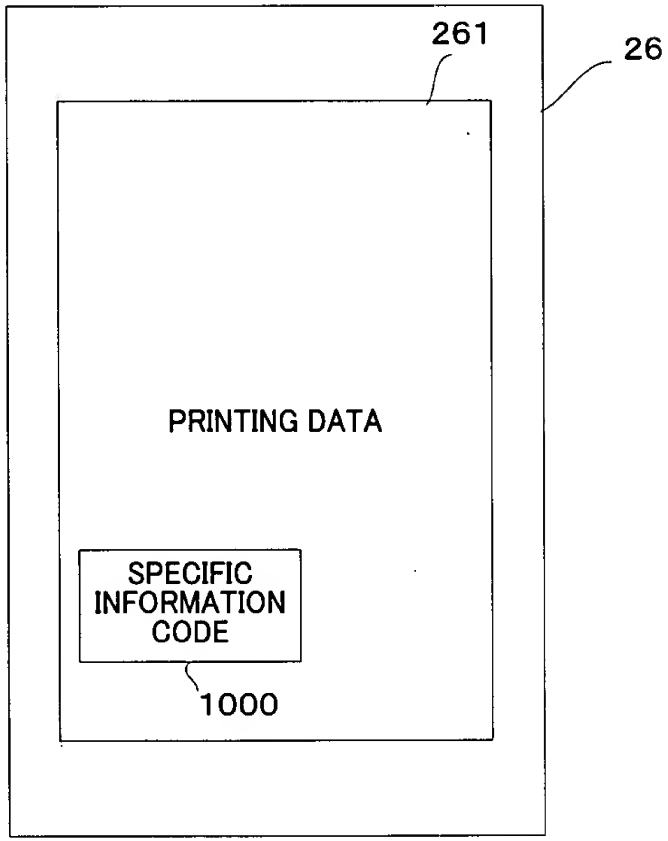


Fig. 8

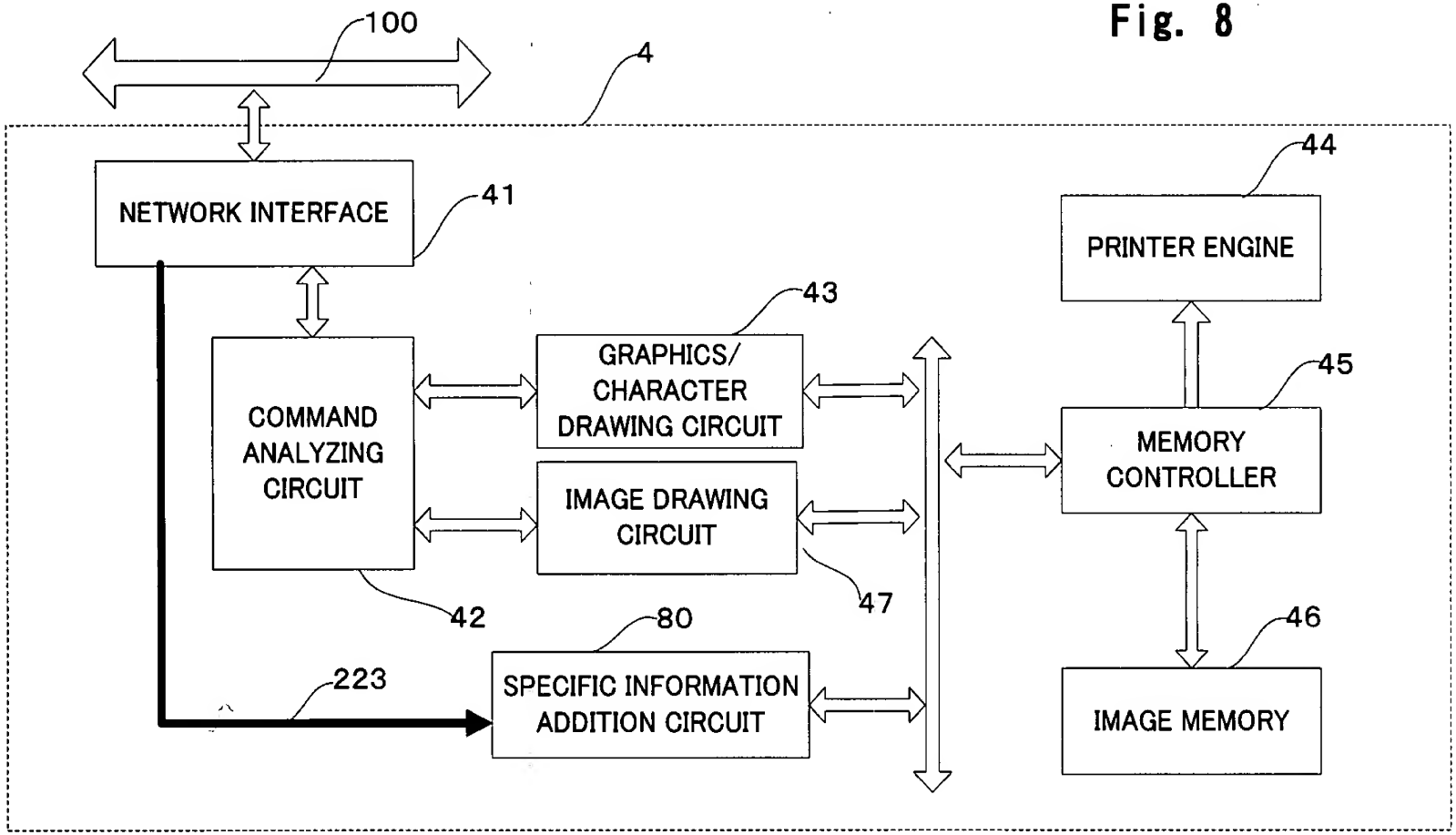
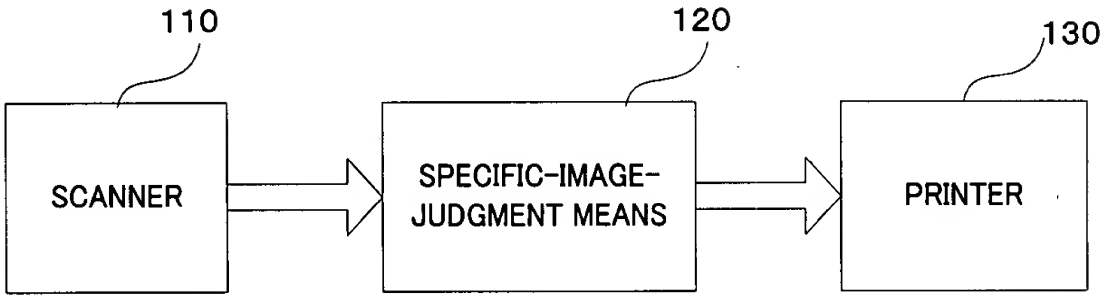

100
4
NETWORK INTERFACE
41
44
PRINTER ENGINE
43
GRAPHICS/
CHARACTER
DRAWING CIRCUIT
45
COMMAND
ANALYZING
CIRCUIT
IMAGE DRAWING
CIRCUIT
MEMORY
CONTROLLER
47
42
80
46
223
SPECIFIC INFORMATION
ADDITION CIRCUIT
IMAGE MEMORY

Fig. 9



[NAME OF THE DOCUMENT] Abstract

[SUMMARY]

[SUBJECT]

This invention relates to a copying apparatus that is capable of quickly preventing and tracking illegal copying.

[SOLVING MEANS]

When printing data 11 are transferred from the personal computer 1 to the printer 2 via the printer driver 12, the printing-information-analyzing circuit 15 monitors the printing data 11, and while checking the image being created in the confirmation memory 16, it compares and analyzes the image with information from the copy-inhibition information 14. In the case that the image created from the printing data 11 is determined to already be registered in the copy-inhibition information 14, an instruction is sent to the printer driver 12 to stop transferring printing data to the printer 2. In this way, illegal copying is prevented before the data are sent to the printer2. Also, information unique to the apparatus is automatically added to the printing data, so it is possible to easily track the copied material.

[SELECTED DRAWING] Fig. 1